UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/718,663	11/24/2003	Jun Furukawa	Q78522	1253

23373 7590 06/24/2008
SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	PAPER NUMBER
2136	
MAIL DATE	DELIVERY MODE
06/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/718,663	FURUKAWA, JUN	
	Examiner	Art Unit	
	PRAMILA PARTHASARATHY	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *8 and 10* is/are allowed.

6)☒ Claim(s) *1-7,9,11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on March 10, 2008. Claims 1 – 11 are pending.

Response to Arguments

2. Applicant's arguments with respect to the rejection(s) of claim(s) 1-11 under obviousness-type double patenting and prior art rejection have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Terao et al. (US Patent 6,651,167). Examiner further directs Applicants attention to Allowed subject matter in section **#11.**

Examiner requests Applicant to provide the English-translation of the cited document in the IDS. Applicant merely states that, "For reference purposes, details of zero-knowledge proof systems are described in ....Sangyo Tosyo Shuppan, "Modern Cryptography" July 30, 1997." (specification Page 2 lines 6-11).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-11 are rejected under 35 U.S.C. 102(e) as being anticipated by Terao et al. (US Patent 6,651,167).

4. As per Claim 1, Terao teaches application view of the invention (Column 15 line 10-Column 16 line 33) and "a generator supplied with a third random tape, for generating a common input and a witness from the third random tape based on a predetermined function (Column 4 lines 33-44; issuing ticket (common input), function based on a secret function, authentication information based corresponding to the ticket);

a simulator supplied with a fourth random tape (Column 4 lines 57-63, interactive device);

a distinguisher supplied with a fifth random tape wherein the generator supplies the common input to the prover, the verifier, the simulator and the distinguisher and supplies the witness to the prover and the distinguisher (Column 4 lines 64-67; the authentication characteristic information generated independently);

a proof history is generated with involving the prover (the user converts the interaction);

a simulated proof history is generated by the simulator without involving the prover (the authentication information and the secret information is not disclosed to the user); and

the distinguisher evaluates the proof system depending on whether a difference in distribution between the proof history and the simulated proof history is computationally indistinguishable for a great majority of possible common inputs and computationally distinguishable for at least one of the possible common inputs" (Column 4 lines 1-17; ticket issuing agency issues interactive devices and distributes to the users with unique secret function and tickets - Common input).

5. As Claims 7, 9 and 11 compare with the limitations of above rejected Claim 1, therefore they are rejected on the same rationale.

6. As per Claim 2, Terao teaches application view of the invention (Column 15 line 10-Column 16 line 33) and "wherein the proof history is generated by the verifier interacting with the prover using the second random tape and the common input, the proof history including the second random tape and the interactive data with the prover, the simulated proof history is generated by the simulator that supplies a sixth random tape to the verifier and interacts with the verifier to simulate interaction between the prover and the verifier, the simulated proof history including the sixth random tape and the simulated interactive data" (Column 4 lines 33-51 and Column 7 lines 2-63; Interactive device generates ticket/information using randomize unit, the calculating unit is used to calculates the secret function unique to the interactive device and the verifier calculate a response based on the information and secret function).

7. As per Claim 3, Terao teaches application view of the invention (Column 15 line 10-Column 16 line 33) and "wherein the prover comprises a proving section and a hash function section, wherein the hash function section inputs data from the proving section and outputs hash data of the inputted data back to the proving section, the proof history is generated by the prover in which the proving section interacts with the hash function section to produce interactive data and hash data of the interactive data is replaced with random data, wherein the proof history further includes data transferred from the prover to the verifier, the simulated proof history is generated by the simulator that simulates interaction between the prover and the verifier based on the common input and the fourth random tape, the simulated proof history including the simulated interactive data" (Column 4 lines 33-51 and Column 7 lines 44-50; the calculation unit that stores secret information unique to the interactive device calculates a hash function computing the hash of the document; Column 11 line 30-52; generating secret function using the hash function which makes attempt to obtain secret function difficult).

8. As per Claim 4, Terao teaches application view of the invention (Column 15 line 10-Column 16 line 33) and "wherein, if for every distinguisher a difference in distribution between the proof history and the simulated proof history is computationally indistinguishable for a great majority of possible common inputs to an extent of an approximately 100% probability and computationally distinguishable for the remaining part of the common inputs, it is determined that the proof system is classified under a weakly computational zero-knowledge proof class" (Column 16 lines 28-33).

9. As per Claim 5, Terao teaches application view of the invention (Column 15 line 10-Column 16 line 33) and "further comprising: a memory for storing an evaluation result of the proof system obtained by the distinguisher, wherein the evaluation result is on public view" (Column 16 lines 15-17).

10. As per Claim 6, Terao teaches "wherein the evaluation result stored in the memory is accessible through a network" (Column 15 lines 10-29).

Allowable Subject Matter

11. Claims 8 and 10 are allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the disclosing in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially disclosing all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-232-4195. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Pramila Parthasarathy/
Primary Examiner, Art Unit 2136
June 23, 2008